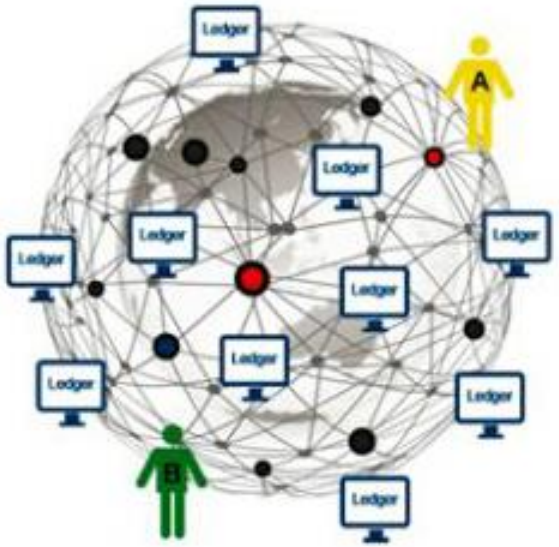
区块链原理及应用简介

目录



前言—比特币的定义及特点

比特币是一种**虚拟货币**（数字货币）。

比特币是一种由开源的P2P软件产生的电子币，数字币，是一种网络虚拟资产。比特币也被意译为“比特金”。比特币基于一套密码编码、通过复杂算法产生，这一规则不受任何个人或组织干扰，去中心化；任何人都可以下载并运行比特币客户端而参与制造比特币；比特币利用电子签名的方式来实现流通，通过P2P分布式网络来核查重复消费。每一块比特币的产生、消费都会通过P2P分布式网络记录并告知全网，不存在伪造的可能。

特点：

1.数字货币。
2.不依托于任何国家或组织而利用计算机技术独立发行。
3.通过P2P分布式技术实现，无中心点。
4.所有人均可自由的参与。
5.总量有限，不可再生。
6.本身机制开源，可以被山寨。

前言—比特币与传统对比：去中心化

传统模式：中心化账本（银行）

银行是一个中心化账本，账本存储在银行的中心数据库，上面写着：张三的A账号余额3000元，李四的B账号余额2000元。当张三想要通过A账号转账1000元给李四的B账号时：

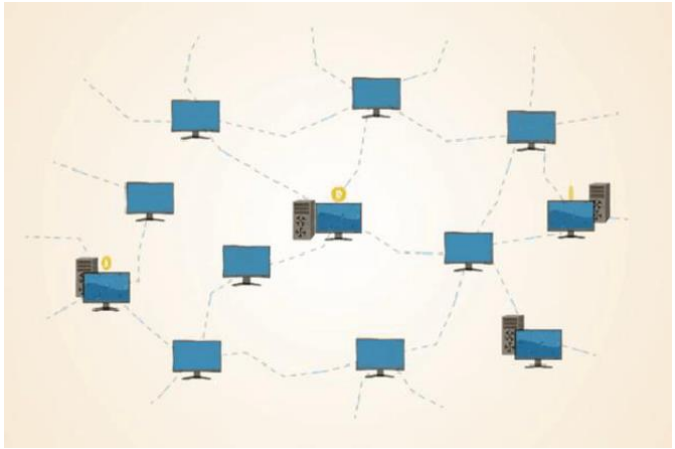
①张三到银行，向银行提交转账要求。
②银行通过银行卡密码等方式确认张三身份，并检查张三的A账号是否有足够余额。
③检查通过后，银行增加一条转账记录：A账号向B账号转账1000元，
并修改余额：A账号余额=3000-1000=2000元，B账号余额=2000+1000=3000元

创新模式：去中心化账本（比特币）

假设有这样的一个小村庄，大家不是靠银行，而是自己用账本来记录谁有多少钱，每个人的账本上都写着：张三的A账号余额3000元，李四的B账号余额2000元。当张三想要通过A账号转账1000元给李四的B账号时：

①张三大吼一声：大家注意啦，我用A账号给李四的B账号转1000块钱。 ②张三附近的村民听了确实是张三的声音，并且检查张三的A账号是否有足够余额。
③检查通过后，村民往自己的账本上写：A账号向B账号转账1000元， 并修改余额：A账号余额=3000-1000=2000元，B账号余额=2000+1000=3000元。
④张三附近的村民把转账告诉较远村民，一传十十传百，直到所有人都知道这笔转账，以此保证所有人账本的一致性。

前言—比特币与传统对比：全部节点参与



比特币用户在电脑上运行比特币客户端软件，这样的电脑称为一个**节点（node）**，大量节点电脑互相连接，形成一张像蜘蛛网一样的**P2P（点对点）网络**。

当张三想要通过A账号转账1比特币给李四的B账号时，当张三想要通过A账号转账1比特币给李四的B账号时：

①张三向周围节点广播转账交易要求：A账号转账1比特币给B账号，并用A账号的私钥签名。（A账号的私钥可简单理解为A账号的密码，只要知道A账号的私钥就能使用A账号上的比特币）
②张三周围的节点通过A账号的公钥检查交易签名的真伪，并且检查张三的A账号是否有足够余额。
③检查通过后，节点往自己的账本上写：A账号向B账号转账1比特币元，并修改余额：A账号余额=3比特币-1比特币=2比特币，B账号余额=2比特币+1比特币=3比特币。
④节点把这个交易广播给周围的节点，一传十十传百，直到所有节点都收到这笔交易。

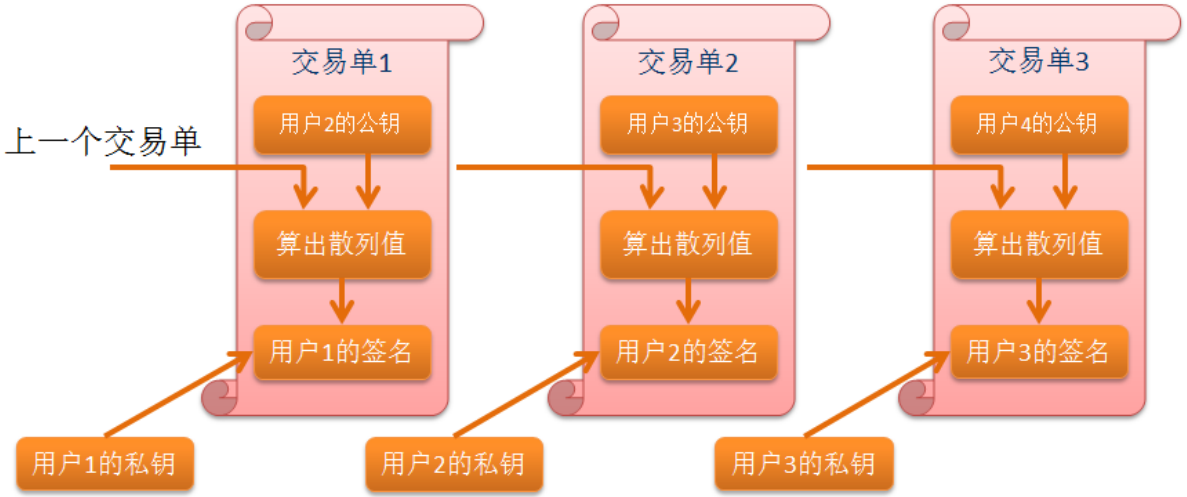
前言—比特币技术原理：交易单

比特币虽然是电子货币，但比特币系统中并没有特定的数据结构用来单纯代表货币。本质上，比特币的存在是通过交易单来提现。通俗的来讲，现实生活中我们有实在的纸张来代表我们的货币（比如面值10块的RMB纸张代表着10块钱RMB），当我们去银行核对财务时银行也提供对账单来表示我们的货币去留。比特币的提现依托于交易单，**交易单类似于银行的对账单，其通过记录货币的去留来证明你有多少货币，而不是提供给你具体的货币单元。**

交易单记录一笔交易的具体信息，比如付款人（交易发起方的公钥）、收款人（交易接收方的公钥）、付款金额（上一笔交易信息）、付款人签名（加密后的Hash值）等。

1 交易单 ID
2 资金来源---上个交易单 ID（张三的钱从哪里来的，比如王二），
3 王二对上一笔资金的签字（证明是王二给张三的）
4 资金去向---李四收款帐号，
5 数额---10 元，
附加张三的签字（每个用户都能够鉴别这是张三签的 10 元交易单，不能伪造）

前言—比特币技术原理：交易签名



数字签名—非对称加密算法

假设有三个交易单，代表用户1给用户2支付钱款“交易单1”，用户2给用户3支付钱款“交易单2”，用户3给用户4支付钱款“交易单3”。

前言—比特币技术原理：区块

sitte@sina.com

Block(块、账簿）：记录交易单的数据单元叫做Block，一个Block上会记录很多交易单。Block有很多份，**每个Block只记录比特币全网10分钟内的交易信息，每约10分钟产生一个新的Block。**每生成一个Block，生产者获得50个比特币奖励，每4年生产出21万个Block后奖励减半。比特币总数2100万个，从2009开始至2140年后生产完毕。

截止2016年9月20号13:17，全网已有**430625**个Block被生产出来，总比特币已达**1800万**以上，总产量已达**85%。**

生产Block的过程，被形象的称为“**挖矿**”，生产工也被称为“**矿工**”。

截至2016年9月20号，全球矿工的全网算力已达**1616P**（ 2016年1月800P ，2015年9月400P ），2013年11月当算力突破100P(百亿亿次，10的18次方)时，已超全球Top500超级计算机总和的9倍还多，目前**已超总和100倍以上。**

前言—比特币技术原理：区块链

Block链：

所有的Block以双向链表的方式链接起来，且**每个Block都会保存其上一个Block的Hash值（这样Block之间的顺序一旦确定就无法更改）**。只有一个Block无上一节点，即：创世Block（第一个Block)。

Block链全网唯一，每个节点都有相同的备份。Block链一旦有更新则全网通知。

前言—比特币历史及相关问题

sitte@sina.com

1. 较大的政策风险，国家组织是否会承认？
   德国：首个承认比特币具有合法货币地位。俄罗斯：对比特币持强硬态度。韩国：拒绝承认比特币的货币地位。荷兰：警告比特币风险。日本：定义比特币为资产。加拿大：承认比特币的货币地位。**泰国**：首个封杀比特币。**美国**：表达了支持的态度。**中国**：不具有货币属性，不是真正意义的货币。

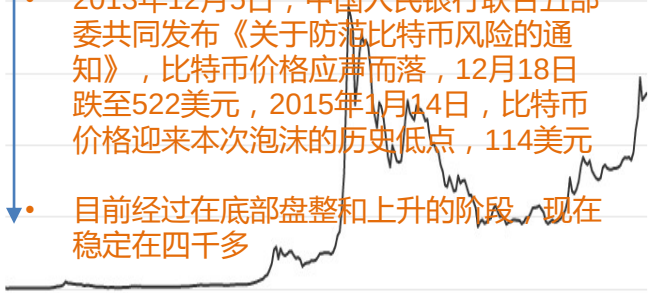
2. 安全性如何得到保证，被盗了谁来给你找回？
   11年MyBitcoin遭遇黑客攻击，7.8W比特币至今下落不明。

3. 总量有限决定了比特币极具投机色彩，价格犹如失控的过山车。
   10年比特币仅为数美分一个，13年3月突破45美元/个，13年11月突破800美元/个。

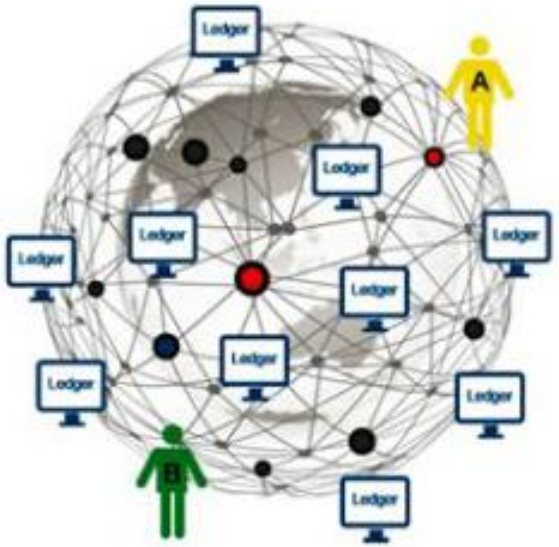
4. 山寨币是否对比特币的生态造成威胁？
   山寨币层出不穷，目前发展的比较好的山寨币有LTC（莱特币）。

5. 比特币本身机制是否存在未发现的致命漏洞？
   比特币机制从目前来看似乎是“精妙绝伦、无懈可击、堪称神作”，但它毕竟仅存在了不到8年（09-16）。

- 08年，一个名为“**中本聪**”的人在网络上发表了一篇论文《**比特币：一种点对点的电子现金系统**》（Bitcoin:A Peer-to-Peer Electronic Cash System）
- 2009年1月3日比特币诞生，2010年5月22日之前前价格为0，2010年8月17日价格为0.0769美分
- 2013年12月4日达到了1147美元的历史高位，在中国的比特币交易平台创下了8000人民币的天价。
- 2013年12月5日，中国人民银行联合五部委共同发布《关于防范比特币风险的通知》，比特币价格应声而落，12月18日跌至522美元，2015年1月14日，比特币价格迎来本次泡沫的历史低点，114美元
- 目前经过在底部盘整和上升的阶段，现在稳定在四千多



目录



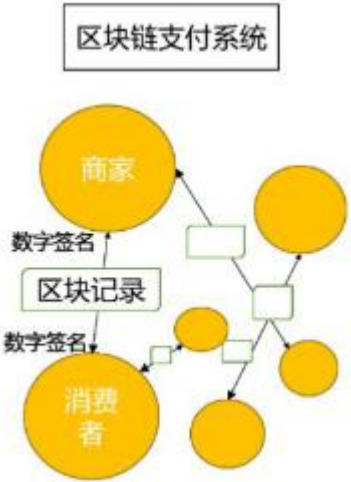
区块链简介—区块链的定义

背景

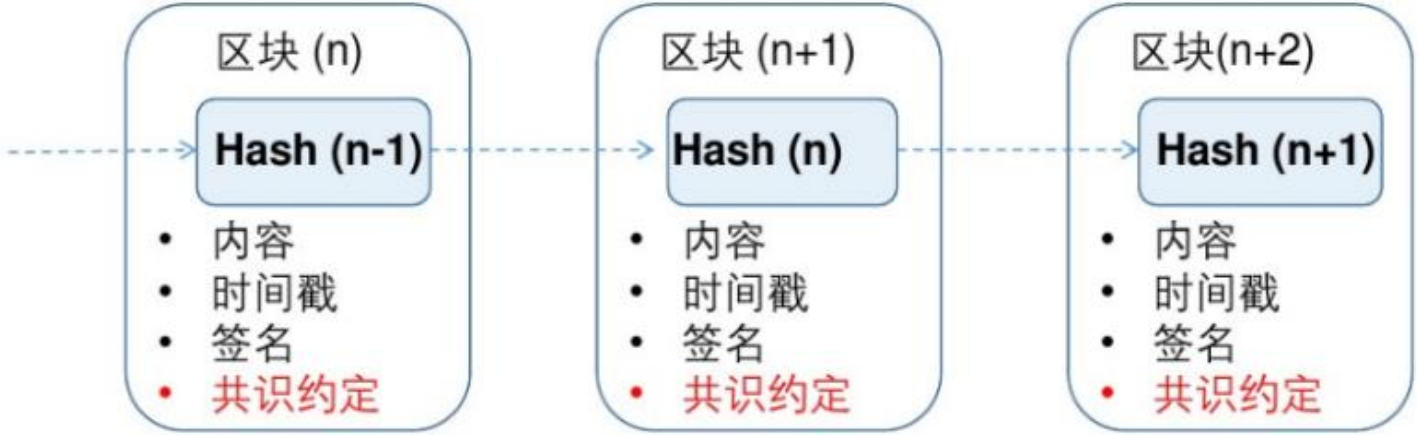
互联网上的交易，几乎都需要借助可资信赖的第三方信用机构来处理电子支付信息。这类系统仍然内生的受制于“基于信用的模式”

区块链

是一个分布式账本，一种通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。它基于密码学原理而不基于信用，使得任何达成一致的双方直接支付，从而不需要第三方中介的参与



区块链简介—区块链的普适原理



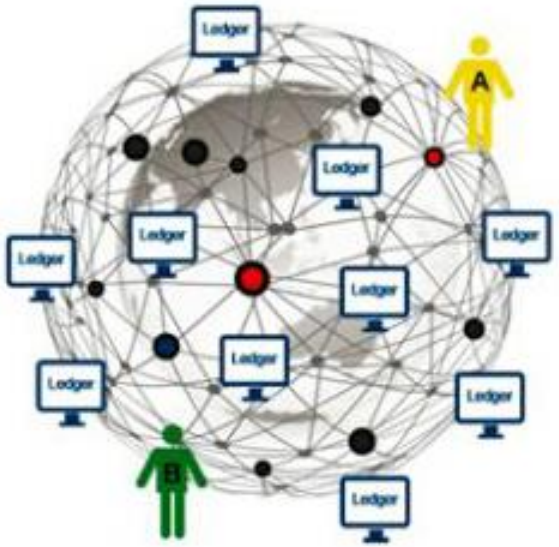
- 当前一切的加密币，一切BlockChain，只是共识约定和存储内容不同
- 比特币是区块链特定共识约定与区块内容的实例体现（内容：交易信息，共识约定：区块时间内加随机数作salt后hash值最大，超50%群体验证）
- 应用区块链技术的过程本质上是**组织区块内容**与**论证共识约定合理性**的过程

区块链简介—创新计算范式

区块链简介—全球关注和重视

- 国际权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等相继报道区块链技术将影响世界。
- 2015年9月创业公司**R3**联合全球顶级银行成立**区块链联盟**，包括摩根大通、美国银行、汇丰银行、花旗银行、富国银行、三菱UFJ金融集团、巴克莱银行、高盛、德意志银行等。目前已达47家联盟成员。
- 2016年4月由中证机构间报价系统股份有限公司等11家机构共同发起的区块链联盟——中国分布式总账基础协议联盟（China Ledger联盟）宣告成立
- 2016年5月中国平安保险(集团)股份有限公司宣布与国际顶尖金融创新公司R3建立了合作伙伴关系，正式加入R3分布式分类账联盟，成为**第一家中国区R3联盟成员。**
- 2016年6月香港友邦人寿保险公司加入R3，成为**第二家中国区成员**；
- 2016年9月继中国平安和香港友邦加入R3区块链联盟之后，中国招商银行成为加入R3的**第三家中国金融机构。**

目录



区块链特征及分类—特征

开放，共识

任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。

交易透明，双方匿名

区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点和节点之间是去信任的，因此节点之间无需公开身份，每个参与的节点都是匿名的。

去中心，去信任

区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需相互信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其他节点。

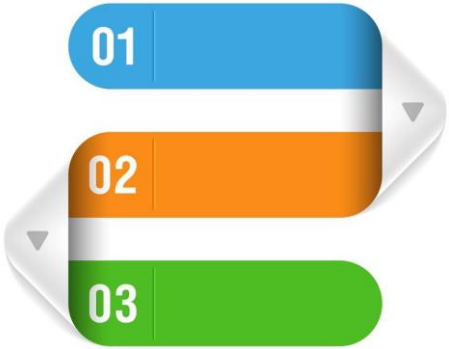
不可篡改，可追溯

单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改，这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

区块链特征及分类—分类

公有链

无官方组织及管理机构，无中心服务器，参与的节点按照系统规则自由接入网络、不受控制，节点间基于共识机制开展工作。



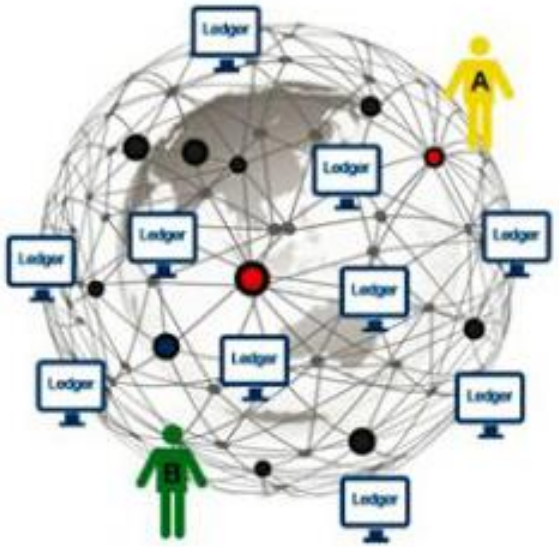
联盟链

由若干机构联合发起，介于公有链和私有链之间，兼具部分去中心化的特征。

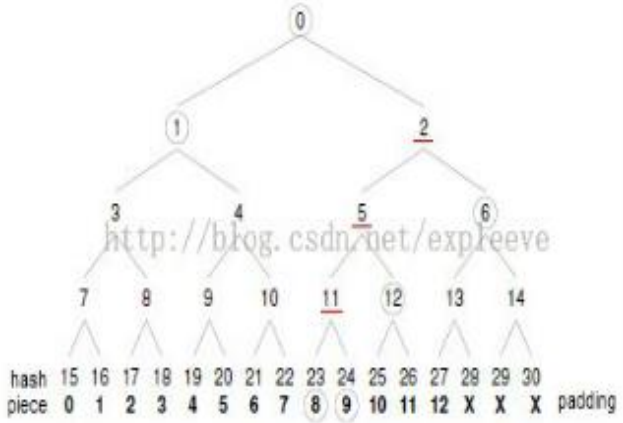
私有链

建立在某个企业内部，系统的运作规则根据企业要求进行设定，修改甚至是读取权限仅限于少数节点，同时仍保留着区块链的真实性和部分去中心化的特征。

目录



区块链网络结构：技术基础



数字签名

数字签名涉及到一个哈希函数、发送者的公钥、发送者的私钥。数字签名有两个作用，一是能确定消息确实是由发送方签名并发出来的。二是数字签名能确定消息的完整性。

SHA256

一种哈希散列函数，可以将任何一串数据输入后得到一个256位的Hash值（散列值）。相同的数据输入将得到相同的结果。输入数据只要稍有变化则将得到一个千差万别的结果，且结果无法事先预知。正向计算十分容易，逆向计算极其困难，在当前科技条件下被视作不可能。

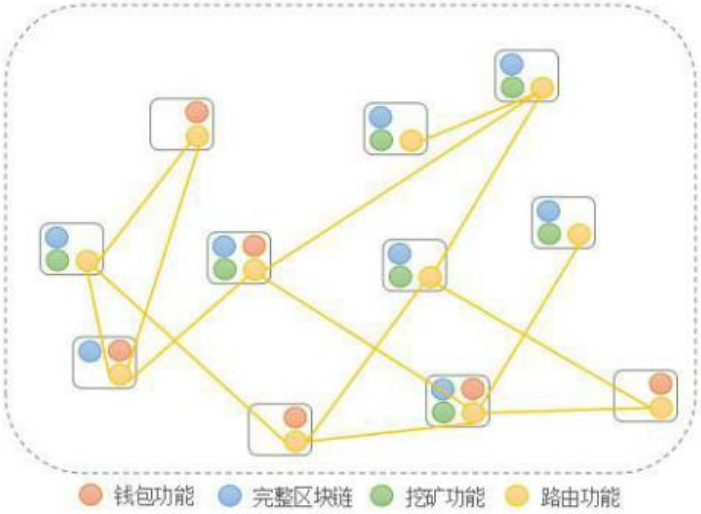
Merkle Tree

一种哈希二叉树，使用它可以快速校验大规模数据的完整性。在比特币网络中，Merkle树被用来归纳一个区块中的所有交易信息，最终生成这个区块所有交易信息的一个统一的哈希值，区块中任何一笔交易信息的改变都会使得Merkle树改变。

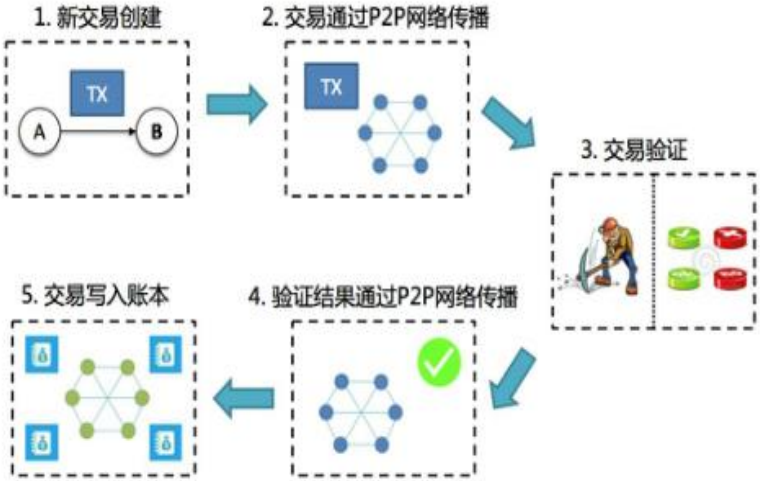
区块链网络结构：节点网络

任何机器都可以运行一个完整的比特币节点，一个完整的比特币节点包括：

1. **钱包**，允许用户在区块链网络上进行交易
2. **完整区块链**，记录了所有交易历史，通过特殊的结构保证历史交易的安全性，并且用来验证新交易的合法性
3. **矿工**，通过记录交易及解密数学题来生成新区块，如果成功可以赚取奖励
4. **路由功能**，必须功能，把其它节点传递过来的交易数据等信息再传送给更多的节点



区块链网络结构：交易过程



第1步：所有者A利用他的私钥对前一次交易（比特币来源）和下一位所有者B（ B以公钥作为接受方地址）签署一个数据签名，并将这个签名附加在这枚货币的末尾，制作成交易单

第2步：A将交易单广播至全网，比特币就发送给了B，每个节点都将收到的交易信息纳入一个区块中（得到6个区块确认后才可使用）

第3步：每个节点通过解一道数学难题，从而去获得创建新区块权利，并争取得到比特币的奖励（新比特币会在此过程中产生）

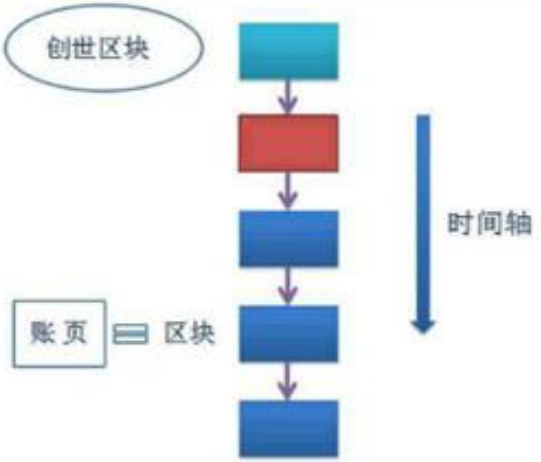
第4步：当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易（取5个节点的中间值），并由全网其他节点核对

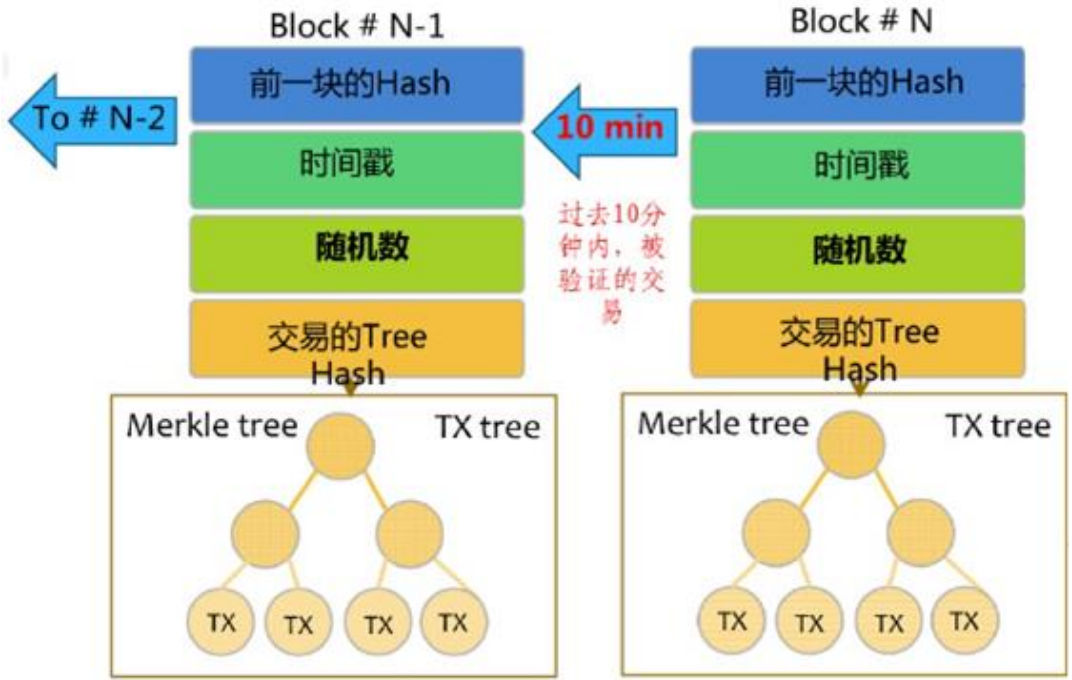
第5步：全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链（约10分钟产生一个，基于最近2016个区块的生成时间自动调整难度值）。

区块链网络结构：数据结构

sitte@sina.com

区块链：全球统一的、公开的数据库，可用于记账

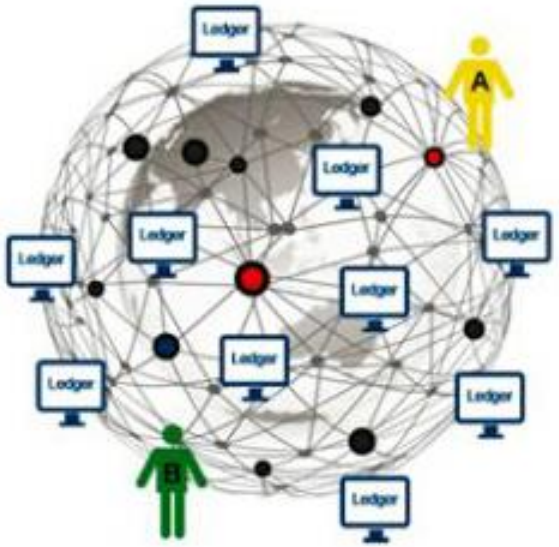




区块链网络结构：区块头

1. **版本号**，标示软件及协议的相关版本信息
2. **父区块哈希值**，引用的区块链中父区块头的哈希值，通过这个值每个区块才首位相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用
3. **Merkle根**，这个值是有区块主体中所有交易的哈希值再逐级两两哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在
4. **时间戳**，记录该区块产生的时间，精确到秒
5. **难度值**，该区块相关数学题的难度目标
6. **随机数（Nonce），**记录解密该区块相关数学题的答案的值

目录



核心问题—工作量证明

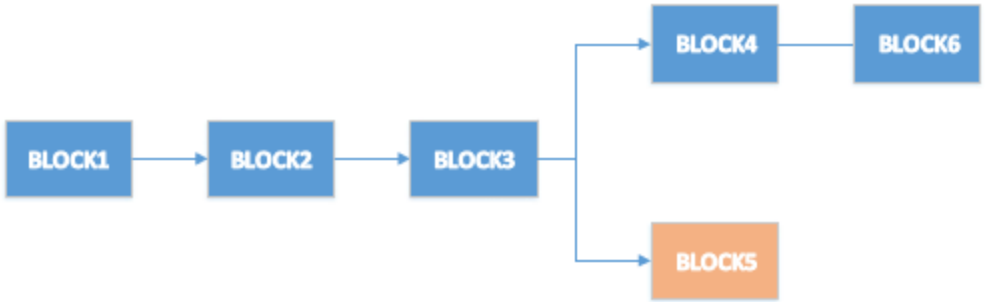
区块头包含一个**随机数**，通过在散列函数中加入这个随机数使得区块的散列值出现了所需的0个数。节点通过反复尝试来找到这个随机数，这样就构建了一个工作量证明机制**PoW**。

PoW机制的本质是cpu一票，“大多数”的决定表达为最长的链，因为最长的链包含了最大的工作量。如果大多数的cpu为诚实的节点控制，那么诚实的链条将以最快的速度延长，并超越其他的竞争链条。如果想要修改已出现的区块，攻击者必须重新完成该区块的工作量外加该区块之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。

核心问题—分叉

同一时间段内全网不止一个节点能计算出随机数，即会有多个节点在网络中广播它们各自打包好的临时区块（都是合法的）。

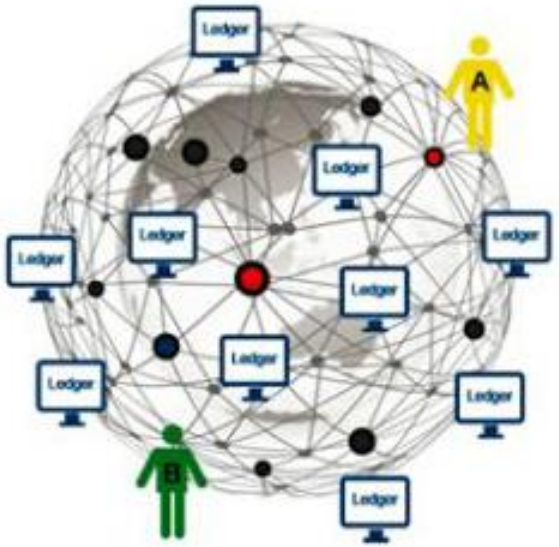
某一节点若收到多个针对同一前续区块的后继临时区块，则该节点会在本地区块链上建立分支，多个临时区块对应多个分支。该僵局的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。其他分支将会被网络彻底抛弃。



核心问题—其他

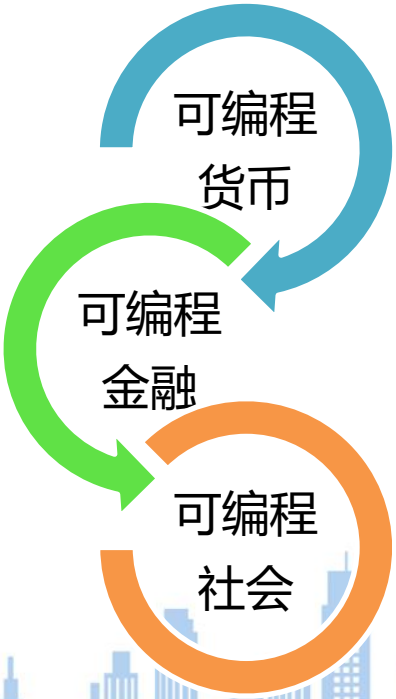
- 双花（即二重支付）
- 高能耗
- 数据库存储空间
- 处理大规模交易的抗压能力
- 安全性
- 无索引大规模数据检索困难
- 智能合约程序表达能力范围
- 去中心化相关问题处理
- 资源消耗问题

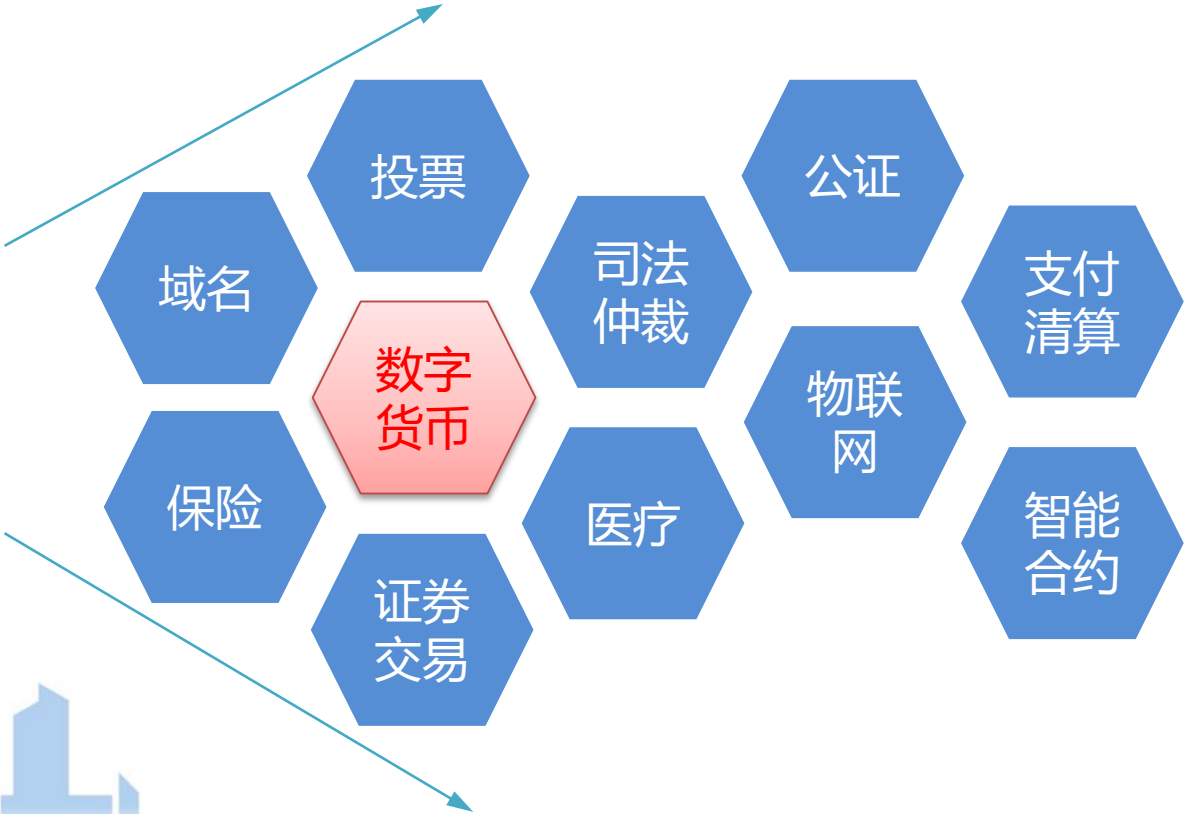
目录



前景展望—万能的区块链

sitte@sina.com

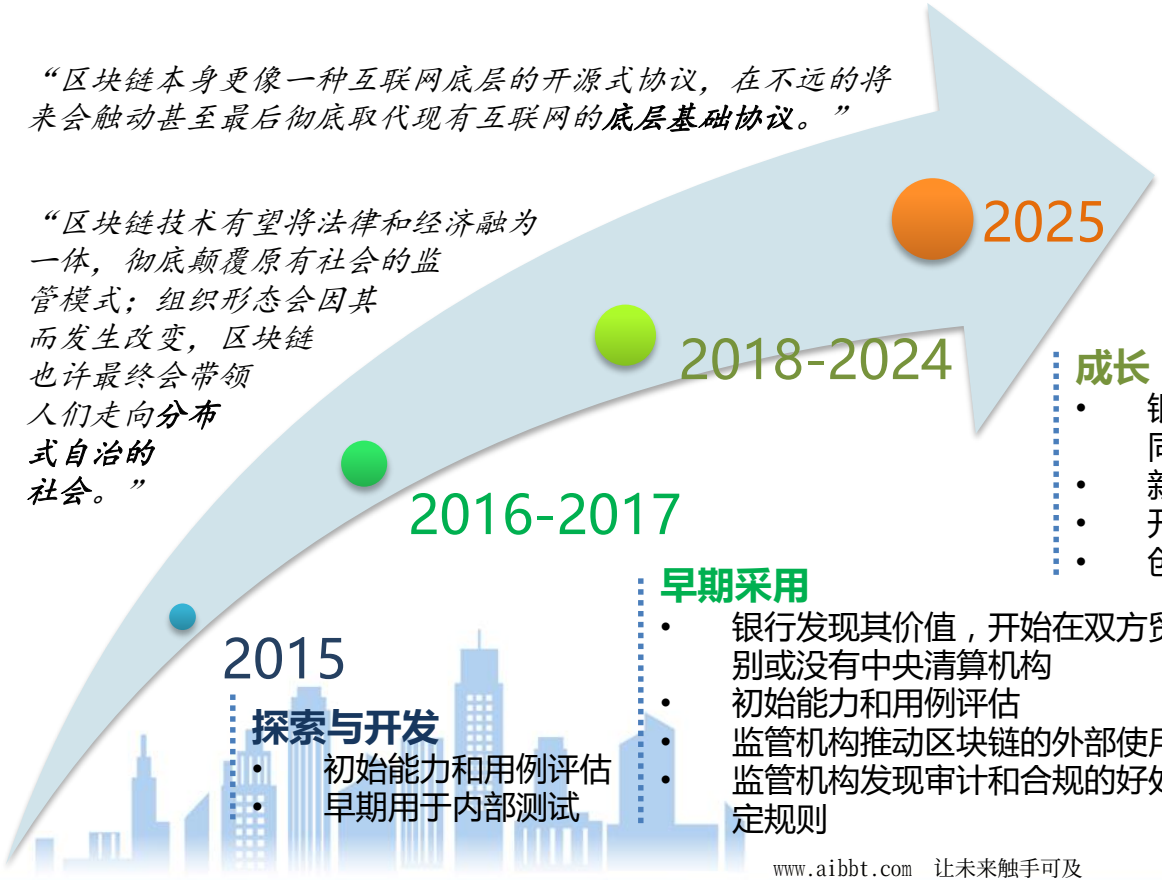




前景展望

*“区块链本身更像一种互联网底层的开源式协议，在不远的将来会触动甚至最后彻底取代现有互联网的**底层基础协议**。”*

*“区块链技术有望将法律和经济融为一体，彻底颠覆原有社会的监管模式；组织形态会因其而发生改变，区块链也许最终会带领人们走向**分布式自治的社会**。”*



2015

探索与开发

- 初始能力和用例评估
- 早期用于内部测试

2016-2017

早期采用

- 银行发现其价值，开始在双方贸易配置资产类别或没有中央清算机构
- 初始能力和用例评估
- 监管机构推动区块链的外部使用案例
- 监管机构发现审计和合规的好处，从而开始制定规则

2018-2024

成长

- 银行开始见证区块链对早期采用者带来的好处，同时制定监管法则，网络影响开始确立
- 新服务提供商和模式开始出现
- 开始疯狂部署大量资产类别
- 创造了新产品/服务，摒弃当前流程和服务

2025

成熟

- 区块链的使用成为主流，同时很好的整合进资本市场体系

sitte@sina.com

THANKS

www.aibbt.com 让未来触手可及